

Appl. No.: 09/690,818
Reply to Office Action of April 30, 2004

Amendment to the Claims

The following listing of the claims supersedes all other listing submitted heretofore.

Listing of the Claims

1. (Original) An access control system for preventing an unauthorized access to a network via a user computer connected to the network, the system comprising;
a memory containing an IP address assigned to the user computer; and
a microprocessor programmed to terminate a connection between the user computer and the network when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory.

2. (Original) The access control system of claim 1, wherein the microprocessor is further programmed to delete the IP address of the user computer from the memory when the originating IP address of the data packet received from user computer does not match the IP address assigned to the user computer that is contained in the memory.

Appl. No.: 09/690,818
Reply to Office Action of April 30, 2004

3. (Original) The access control system of claim 1, wherein the microprocessor is further programmed to update the IP address of the user computer contained in the memory.

4. (Original) The access control system of claim 1, wherein the memory is a part of the microprocessor.

5. (Original) An access control system for preventing an unauthorized access to a network via a user computer connected to the network through a host computer system, the system comprising:

a memory containing an IP address assigned to the user computer; and
a microprocessor programmed to terminate a connection between the user computer and the host computer system when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory,

wherein the access control system is located between the user computer and the host computer system.

6. (Original) The access control system of claim 5, wherein the microprocessor is further programmed to delete the IP address of the user computer from the memory when the originating IP address of the data packet received from the user computer

Appl. No.: 09/690,818
Reply to Office Action of April 30, 2004

does not match the IP address assigned to the user computer that is contained in the memory.

7. (Original) The access control system of claim 5, wherein the microprocessor is further programmed to update the IP address of the user computer contained in the memory.

8. (Original) The access control system of claim 5, wherein the memory is a part of the microprocessor.

9. (Original) A method for preventing an unauthorized access to a network via a user computer which is connected to the network and to an access control system, the method comprising:

storing an IP address of the user computer in a memory of the access control system;

receiving a data packet from the user computer;

comparing an originating IP address of the data packet with the IP address of the user computer stored in the memory of the access control system; and

denying the user computer an access to the network if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

Appl. No.: 09/690,818
Reply to Office Action of April 30, 2004

10. (Original) The method of claim 9, wherein the denying step includes terminating the connection between the user computer and the network.

11. (Original) The method of claim 9, further comprising updating the IP address of the user computer stored in the memory of the access control system.

12. (Original) The method of claim 9, further comprising deleting the IP address of the user computer from the memory of the access control system if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

13. (Original) A method of preventing an unauthorized access to a network via a user computer connected to the network through a host computer system which is connected to an access control system, the method comprising:

storing an IP address of the user computer in a memory of the access control system;

receiving a data packet from the user computer;

comparing an originating IP address of the data packet with the IP address of the user computer stored in the memory of the access control system; and

terminating a connection between the user computer and the host computer

Appl. No.: 09/690,818
Reply to Office Action of April 30, 2004

system if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

14. (Original) The method of claim 13, further comprising deleting the IP address of the user computer from the memory of the access control system if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

15. (Original) The method of claim 13, further comprising updating the IP address of the user computer stored in the memory of the access control system.

16. (Currently Amended) A secure network comprising:
a host computer system connected to the secure network;
an access control system connected to the host computer system and having a memory; and

a user computer connected to the host computer system ~~capable of accessing~~
and configured to access the secure network through the host computer system,
wherein the memory of the access control system is programmed to terminate a connection between the host computer system and the user computer when an originating IP address of a data packet sent from the user computer for transmission to a node in the secure network does not match the IP address of the user computer

Appl. No.: 09/690,818
Reply to Office Action of April 30, 2004

contained in the memory of the access control system.

17. (Original) The secure network of claim 16, wherein the user computer and the host computer system are connected via a Public Switched Telephone Network.

18. (Original) The secure network of claim 16, wherein the host computer system comprises an access server and a plurality of modems and wherein the access control system is located between the access server and the plurality of modems.

19. (Original) The secure network of claim 16, wherein the host computer system and the user computer are connected via a local area network.

20. (Original) A secure network comprising:
a user computer connected to the secure network; and
an access control system connected to the user computer and having a memory,
wherein the memory of the access control system contains an IP address
assigned to the user computer, and wherein the access control system is programmed
to deny the user computer an access to the secure network when an originating IP
address of a data packet sent from the user computer for transmission to a node in the
secure network does not match the IP address of the user computer contained in the
memory of the access control system.

21. (Currently Amended) An access control system for preventing an unauthorized access to a network via a user computer connected to the network, the system comprising:

a memory containing an IP address assigned to the user computer; and
a comparator structure ~~capable of terminating~~ configured to terminate a connection between the user computer and the network when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory.

22. (Original) The access control system of claim 21, wherein a comparator structure comprises a microprocessor.

23. (Original) The access control system of claim 22, wherein the memory is a part of the microprocessor.